𝒟FW

In re: Application of	Victor Gorelik
Application No.	10/725,116
Filed	12-02-2003
Title	TWISTED SIGNATURE
Examiner	LOUIE, OSCAR A
Art Unit	2136

Reply Brief

Table of Contents

1

Status of Claims.

Originally I have made 6 claims. Claims 1-6 have the status as follows.

Claim 1 (Original): A method for securely submitting biometric data from a client to a server comprising the steps of:

performing sampling of a real biometric characteristic at the client; and

shuffling arrays of real biometric characteristics in the sequence known at client only to thereby generate twisted biometric data; and

submitting the twisted biometric data from the client to the server.

Claim 2 (Original): A method according to claim 1 wherein the shuffling sequence is calculated at client on the base of the value of a secret object created at the client and known to client only.

Claim 3 (Original): A method according to claim 2 combined with the step of multiplying the arrays of biometric characteristics by the sequences of numbers fixed for each type of array and known at the client only.

Claim 4 (Original): A method according to claim 3 wherein the step of submitting of twisted biometric data is followed by the step of comparing this data against the samples of twisted biometric data saved at the server previously, in such a way, that the result of the verification and/or identification depends neither on the specific sequence in which biometric arrays were shuffled on the client, nor on the specific sequence of numbers used on the client to change the values of the arrays.

Claim 5 (Previously presented): A system for secure use of biometric data comprising: the means for performing twisted sampling by changing the sequence of terms in biometric array and submitting data to the server, said system programmed for performing verification and/or identification of the client.

Claim 6 (Canceled).

Grounds of rejection to be reviewed on appeal

Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Buffam (US-6185316-B1) in view of Scheidt at al ("Scheidt")(US-6542608-B2).

Claims 1-5 are the appealed claims.

Argument.

In his Answer (mailed 3/27/2008) to my Appeal Brief the Examiner states that I failed "over the claim language".

I believe that there is a very important difference in the claims. It is the difference between infinite number of possible transformations in my application and big, but limited number of transformations in Buffam's and Scheidt's inventions.

My claim 3 contains the step of "multiplying the arrays of biometric characteristics by the sequences of numbers". It creates infinite number of possible transformations, because even one multiplier can have infinitely many values.

Buffam inserts several "false image points"; Scheidt claims "randomization of digital string". Both methods create big, but limited number of possible transformations.

This number is so big that from the practical point of view it is considered as infinite. This consideration may be true from the point of view of breaking security of server. However the situation is different when the security of server is already breached (no matter how) and the attacker is trying to restore the biometrics of the customer.

In this case attacker has additional information including the way how biometric points were registered. In my simplified example, see the Appeal Brief, N points are located on the circle. So, if the attacker finds one reverse transformation that has 4 points not located on the circle, he avoids examining all the other transformations with different positions of the rest (N-4) points. As a result, the problem of restoring biometric information becomes solvable under Buffam and Scheidt and it is explicitly unsolvable in my approach.

That is why I believe that the difference between my "multiplying the arrays of biometric characteristics by the sequences of numbers" and Scheidt's "randomizing of digital string" or Buffam's "false image points" is important from the point of view of the claim language.

If my argument looks reasonable, but the Board decides that the claim language should be amended to overcome rejection, I would appreciate the advice of the Board.

Inventor   5.5.2008   V.Gorelik.